

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK USER ID 100001810378861
THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK INC.,
HEADQUARTED AT 1601 WILLOW
ROAD, MENLO PARK, CA 94025

Case No. 3:19-MJ- 1006

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, John Williams, Jr., an Investigator with the Knoxville Police Department (KPD) Internet Crimes against Children (ICAC) Task Force and being a Task Force Officer with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), being duly sworn, deposes and states the following:

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user IDs.

2. I have been employed with the Knoxville Police Department since August 14, 2000. Since December 2012, I have been assigned to the KPD's ICAC Task Force as an

undercover online investigator. The KPD-ICAC Task Force is responsible for investigating and enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United States Code, Chapter 110, including, without limitation, sections 2251(a), and 2252A(a)(5)(B). I have acquired experience in these matters through specialized training and everyday work related to these types of investigations.

3. As a federal task force officer, I am authorized to investigate violations of the laws of the United States, and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. The information contained within the affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of a search warrant, I have not included each and every fact known to me concerning the investigation. I have received training in the area of sexual exploitation of minors, including the enticement of minors by adults to engage in sexual activity.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251(a), and 2252A(a)(5)(B) have been committed by ANDREW ODELL OVERHOLT. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

6. On January 11, 2019, I received a Cybertip 45476094 from the National Center for Missing and Exploited Children (NCMEC) regarding Facebook communications. The

Cybertip indicated a current or imminent risk to an 8 year-old male child as well as production and distribution of child pornography.

7. NCMEC reported that a 28-year-old male, Andrew Odell Overholt appeared to be producing and distributing apparent Child Exploitation images (CEI) via Facebook Messenger. Conversations provided by Facebook to NCMEC indicated that the Andrew Odell Overholt may have access to [REDACTED]. In addition, based on the Facebook messages, it appeared that Andrew Odell Overholt had engaged in sexual activity with the [REDACTED] and produced pornographic images [REDACTED].

8. Specifically, Cybertip 45476094, wherein Facebook provided conversations between the Facebook unique identifier accounts (UID) of Andrew Odell Overholt (UID 100001810378861) and Braxton Mills (UID 100012361382799). And communications between Andrew Odell Overholt (UID 100001810378861) and Hailey Ison (UID 100002171022404).

9. According to the Cybertip, on August 22, 2018, between 9:49:51am PDT and 11:08:20pm PDT, communication occurred between Andrew Odell Overholt (UID 100001810378861) and Hailey Ison (UID 100002171022404). During this communication Andrew Odell Overholt provided Hailey Ison with his phone number, [REDACTED], and communicated he had sexually assaulted [REDACTED].

10. Further, in the communication, Andrew Odell Overholt and Hailey Ison make plans to meet in order for Hailey Ison to have sexual contact with [REDACTED] in exchange for sexual contact between [REDACTED] and Andrew Odell Overholt.

11. On August 25, 2018, between 7:42:35pm PDT and 10:54:39pm PDT, the Cybertip showed communication occurred between Andrew Odell Overholt (UID 100001810378861) and Braxton Mills (UID 100012361382799). During this Facebook Messenger communication, Andrew Odell Overholt is following instruction from Braxton Mills to produce pornographic images [REDACTED] Andrew Odell Overholt produces the requested pornographic images [REDACTED] and sends them to Braxton Mills via the Facebook Messenger service.

12. During this communication Andrew Odell Overholt produced numerous pornographic images of himself [REDACTED] The images are of [REDACTED] [REDACTED] during the production of these images. Below is a description of two of those image files:

1) 7af7s476j24g8gws40118813_297697047680535_8855007685607686144

_o.jpg – This file is a color image that is 37.5KB in size. The image depicts [REDACTED]
[REDACTED]

Andrew Odell Overholt is wearing a black t-shirt and standing over the child and holding his penis inches away from the child's mouth.

2) c5uue11k7a8k08sk40097764_715049398836023_134601158198873292

8_o.jpg – This file is a color image that is 31.2KB in size. The image depicts [REDACTED]
[REDACTED]

[REDACTED] Andrew Odell Overholt is standing over the child with his penis on the child's buttocks.

13. Facebook provided the following information for the account of Andrew Odell Overholt.

- a. Account - Andrew Overholt
- b. Mobile Phone - [REDACTED]
- c. DOB - [REDACTED]
- d. Approximate age - 28
- e. Email address - [REDACTED]
- f. Screen name - Andrew.overholt.9
- g. ESP User ID- 100001810378861

14. On January 11, 2019 I contacted the school resource officer at [REDACTED]

[REDACTED] TN. I was able to confirm that [REDACTED]

[REDACTED] I also confirmed that the phone number [REDACTED] that Facebook provided as the phone number associated with Andrew Odell Overholt's Facebook account is the same phone number [REDACTED]. Additionally the school resource officer provided an address of [REDACTED] TN [REDACTED] for Overholt [REDACTED]

15. I accessed the Tennessee Criminal Justice Portal and located an Andrew Odell Overholt. Information revealed that an Andrew Odell Overholt with a date of birth of [REDACTED] resided at the address of [REDACTED] TN [REDACTED]

16. On January 11, 2019, Investigators went to [REDACTED], TN. Investigators located Andrew Odell Overholt and asked him if he would speak with investigators in relation to his Facebook account. Andrew Odell Overholt stated that he would speak with investigators regarding his Facebook account and stated, "it got hacked". Andrew

Odell Overholt was mirandized and initialed and signed a Knoxville Police Department rights waiver form.

17. Investigators showed the messages that were provided by Facebook to Andrew Odell Overholt. Andrew Odell Overholt advised, "That's my Facebook". Investigators also showed Andrew Odell Overholt the images that were provided by Facebook and asked him if the images were of him. Andrew Odell Overholt responded, "Yeah." Andrew Odell Overholt further stated it was his penis in the images and the child in the images [REDACTED]

18. On January 11, 2019, Investigators submitted a request to Facebook to preserve all content related to Facebook (UID 100001810378861).

19. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

20. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

21. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request"

accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

22. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

23. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

24. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It

also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video.

When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

25. Facebook users can exchange private messages on Facebook with other users.

Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

26. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

27. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

28. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

29. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log

includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

30. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

31. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

32. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

33. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts

between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

34. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the

offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

35. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

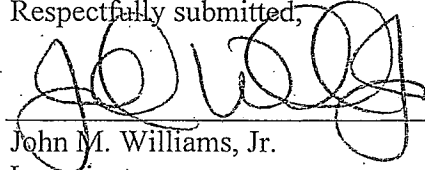
CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant.

38. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



John M. Williams, Jr.

Investigator

Knoxville Police Department

Internet Crimes Against Children Task Force

Subscribed and sworn to before me on this 28th day of January, 2019



DEBRA C. POPLIN

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook user **100001810378861** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including **for user ID 100001810378861**: full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities **from the creation date of the account or July 2, 2010, whichever date is later through January 11, 2019**;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have the users tagged in them **from the creation date of the account or July 2, 2010, whichever date is later through January 11, 2019**; including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including

the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user **from the creation date of the account or July 2, 2010, whichever date is later through January 11, 2019**; including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
- (g) All "check ins" and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (j) All information about the Facebook pages that the account is or was a "fan" of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the account **from the creation date of the account or July 2, 2010, whichever date is later through January 11, 2019**;

- (m) All information about the user's access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;
- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within **14 DAYS** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2422(b), 2251(a), and 2252A(a)(5)(B) involving **ANDREW ODELL OVERHOLT from the creation date of the account or July 2, 2010, whichever date is later through January 11, 2019**; including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence of the communications between Andrew Odell Overholt, Hailey Ison and Braxton Mills as it relates to the crime under investigation;
- (b) Evidence of the digital files sent and received as it relates to the crime under investigation;
- (c) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Facebook, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Facebook. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Facebook, and they were made by Facebook as a regular practice; and
- b. such records were generated by Facebook's electronic process or system that produces an accurate result, to wit:
 1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Facebook in a manner to ensure that they are true duplicates of the original records; and
 2. the process or system is regularly verified by Facebook, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature